

Smart positioners in safety instrumented systems

A review of the way microprocessor-based digital valve controllers – otherwise “smart positioners” – can improve the capabilities of safety systems in detecting potential risks and heading them off before they become a danger

Riyaz Ali and LeRoy Jero

Fisher Controls International LLC

The operation of many industrial processes, especially those within the chemical and oil and gas industries, involves inherent risk due to the leaking of dangerous chemicals or gases. Safety instrumented systems (SIS) are designed specifically to protect personnel, equipment and the environment by reducing the likelihood or the impact of an identified emergency.

These safety systems involve final control elements such as emergency shutdown valves, emergency venting valves, emergency isolation valves, critical on-off valves etc. These valves are not continually moving, like a typical control valve, but normally remain in one position and are expected to operate reliably when an emergency occurs.

Valves that remain in one position for long periods are subject to becoming stuck in that position and may not operate when needed. This could result in a dangerous condition leading to an explosion, fire, and/or a leak of lethal chemicals and gases. To ensure the needed reliability and availability of valves in safety systems, they need to be tested frequently.

Unfortunately, the traditional method of testing these safety valves requires that the plant be shut down, or alternatively that the safety system be rendered inoperable during the time that the valves are being tested. These are both very undesirable and very expensive options. This article reviews this safety problem in detail, and then shows

how digital valve controllers can be used to improve the reliability of safety systems as well as providing a multitude of additional advantages.

The problem

Typically, safety instrumented systems consist of three elements:

1. Sensors that collect information necessary to determine if an emergency situation exists. These sensors are dedicated to SIS service and have process taps which are separate and distinct from the normal process information gathering system.

2. A logic solver that determines what action is to be taken based on the information gathered by the sensors. Highly reliable logic solvers are used to provide both fail-safe and fault-tolerant operation.

3. A final control element that implements the action, if any, required by the logic solver. The final control element is typically a pneumatically actuated valve.

Obviously, it is imperative that all three elements must function as designed in order for the SIS to take the process to a safe condition.

One of the first tasks of the SIS designer is to perform a risk-tolerance analysis to determine what level of safety is needed. Performing a risk-tolerance analysis involves:

1. Identifying the hazards. Hazards can be identified using a number of different techniques. Software programs are available to

assist in HAZOP analysis.

2. Assessing the risk associated with each of the identified hazards. In other words, how potentially significant is each hazard and how often is it expected to occur?

3. Considering other independent protection layers (IPL) that may be in place.

A risk factor must then be determined for each of the identified hazards. Risk is a function of the probability (likelihood or frequency) and consequences (severity) of each hazardous event. Table 1 presents five different levels of risk that are based on frequency of occurrence.

Table 2 illustrates another five levels of risk that are based on severity of the occurrence.

The analyst can also take into account the severity of potential environmental consequences and/or financial losses due to lost production or equipment damage.

IEC and ISA standards specify precise levels of safety that must be obtained and further demand that plants furnish quantifiable proof of compliance. These standards use safety integrity levels (SIL) to quantify safety performance targets for safety instrumented systems.

The IEC standards describe four possible discrete SILs while the ISA standard considers only the three levels shown in Table 3. SIL4 has restricted applications, such as nuclear, aromatics etc. Generally, most process applications lie within the levels of SIL1 or SIL2, with SIL3 applying to critical

Risk level factors based on frequency		
Risk level	Descriptive word	Frequency of occurrence
5	Frequent	One per year
4	Probable	One per 10 years
3	Occasional	One per 100 years
2	Remote	One per 1000 years
1	Improbable	One per 10 000 years

Table 1

Risk level factors based on severity		
Risk level	Descriptive word	Potential consequences to personnel
5	Catastrophic	Multiple deaths
4	Severe	Death
3	Serious	Lost time accident
2	Minor	Medical treatment
1	Negligible	No injury

Table 2

Safety integrity levels: target failure measures

Safety integrity level (SIL)	Risk reduction factor (RRF)	Average probability of failure on demand (PFD)
1	10 to 100	0.1 to 0.01
2	100 to 1000	0.01 to 0.001
3	1000 to 10 000	0.001 to 0.0001

Table 3

applications. The total overall risk can be determined by multiplying the risk level factors together from Tables 1 and 2 to obtain a product from 1 to 25. If this product falls between 15 and 25, the risk is considered high and would indicate a possible need for a SIL3. If the product is 6 or less, the risk is considered low. Risk is deemed moderate between 6 and 15, and high when above 15.

This type of analysis needs to be performed for each hazardous event for each safety function. Once this is done, the analyst then needs to consider the level of protection that may be provided by other independent protection layers (IPL) such as basic process control functions, alarms and operator intervention; physical protection such as relief devices or dikes, plant emergency response measures, community emergency measures plus others.

Taking all these factors into consideration, the analyst then can assign an overall SIL target level. It is then up to the designer to instrument a SIS that will provide the required safety integrity level.

The safety integrity level of the SIS is a function of its probability of failure on demand (PFD). Safety instrumented systems with the lowest average PFD provide the highest safety integrity level, as shown in Table 3. Some safety analysts often like to refer to a risk reduction factor (RRF) which is simply the reciprocal of the PFD.

There are two basic ways for SIS systems to fail, and by understanding these it is possible to calculate a probability of failure on demand.

The first way is commonly called a nuisance or spurious trip, which usually results in an unplanned but safe process shutdown. While, typically, there is no danger associated with this type of SIS failure, the operational costs can be enormous.

The second type of failure does not cause a process shutdown nor a nuisance trip. Instead, it remains undetected, permitting continued process operation in an unsafe and dangerous manner. Should an emergency demand occur, the safety system would be unable to respond properly. These

failures are known as covert, or hidden, failures, and they contribute to the probability (PFD) of the system failing in a dangerous manner.

The PFD for the safety system is the sum of PFD for each element of the system. To determine the PFD of each element, the analyst needs documented, historical failure rate data.

This failure rate is used in conjunction with the test interval (TI) term to calculate the PFD. It is this test interval that accounts for the length of time before a covert fault is discovered through testing.

Lengthening the interval between tests directly impacts on the PFD value in a linear manner (if you double the interval between tests, you double the PFD and make it twice as difficult for the system to meet the target SIL).

The conventional solution

Estimates indicate that as much as 40 to 50% of loop operating problems are caused by final control elements. Therefore it is imperative that these valves be tested frequently in order to reduce the PFD and meet the target SIL. The more frequently the valves are tested, the less likely they will be to fail.

The only sure way to test a final control element completely is with an in-line test that strokes the valve from 0–100% (full open/full close). Unfortunately, to stroke a shutdown valve completely often requires a total shutdown of the process, causing a significant loss in production. Operations managers usually wait to test the valves until a scheduled plant shutdown.

In the past, plant turnarounds were scheduled every two to three years. However, with increased system reliability and more inclusive preventive maintenance programmes, plant turn-arounds now are being scheduled to occur every five to six years. Although extended periods between turnarounds improve economic returns by increasing production, they also mean that safety system final control elements are tested less frequently. This has a dramatic impact on the PFD of the system, which often prevents it from meeting the target SIL.

In an attempt to get around this problem, many companies have devised methods for testing SIS valves online so they do not have to shut down the process. The typical

approach is to install a bypass around each safety valve. Although bypassing the safety valve during testing is done to improve the PFD, not all of this testing approach goes to that benefit. The fraction of time that the system remains in bypass must be taken into account in the PFD calculation. For long bypass periods or frequent testing, the negative impact on PFD can be significant to where it could negate much of the benefit obtained by the testing.

Safety engineers recognise that the most likely failure mode of a discrete shutoff valve is that it remains stuck in its normal standby position. Testing for this type of failure requires stroking the valve only a small amount to verify that the valve is not stuck. This partial-stroke technique can detect a large percentage of covert valve failures. Furthermore, performing this type of test online without shutting down the process could improve the PFD without a loss of production.

Over the years, a variety of partial testing methods have been developed. While all of them have a definite risk of spurious shutdown trips, limiting valve travel using a mechanical device seems to be the most popular. Mechanical limiting methods may involve a pin, a valve stem collar, a valve handjack, or some other apparatus that restricts valve travel to 15% or less of full stroke.

While these mechanical limiting devices themselves are inexpensive, the pneumatic test panels used to conduct the test are complex and costly. The testing process must be manually initiated in the field, and the tests themselves are manpower-intensive and subject to error. In addition, a major drawback is that the safety shutdown function is not available during the test period. Likewise, there is always the possibility that the safety valve will be left inadvertently in a mechanically-limited condition.

Worse yet, this situation cannot always be determined by a casual inspection. This means that the valve potentially could be out of service for an extended period of time with the operators being unaware of the situation.

Smart positioners

So-called “smart” positioners have grown in great popularity in recent years. These are microprocessor-based, current-to-pneumatic digital valve controllers that are communicating instruments with internal logic capability. In addition to the traditional

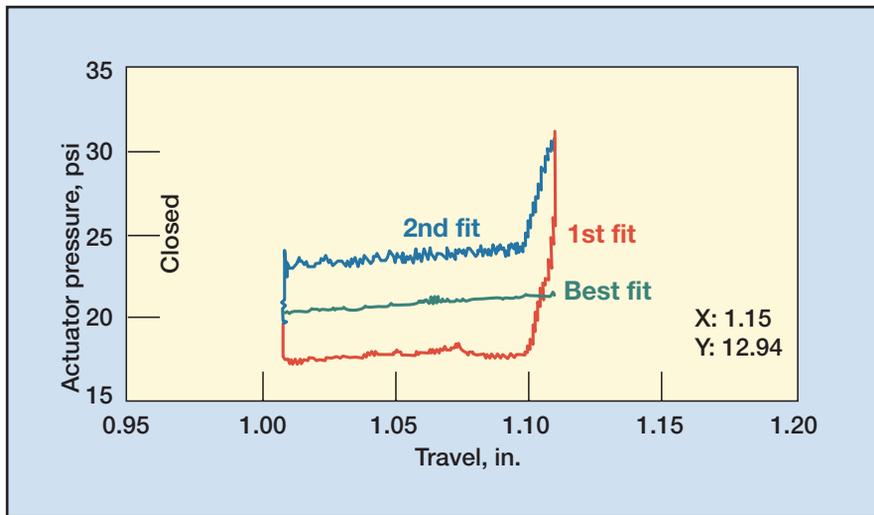


Figure 1 Valve signature test and analysis on an SIS valve, identifying packing problems, leakage in the pneumatic path to the actuator, valve sticking, actuator spring rate and bench set

function of converting a current signal to a pressure signal to operate the valve, these smart positioners use the HART communications protocol to give easy access to information that is critical to process operation.

In addition to this, the smart positioner receives feedback about valve travel position plus existing supply and actuator pneumatic pressures, which allows it to diagnose not only itself, but also the valve and actuator to which it is mounted.

Including a smart positioner as part of the final control element facilitates on-line, partial-stroke testing without the need for special mechanical limiting devices or other special test apparatus. Because the positioner communicates via HART protocol, the partial-stroke test can be initiated from a HART hand-held communicator, from a personal computer running the positioner companion software, or from a panel-mounted pushbutton hardwired to the positioner terminals. Since the testing sequence

is completely automatic, it eliminates errors and possible nuisance trips. For safety reasons, the operator is required to initiate the test sequence.

The partial-stroke technique along with the automated routine provided by the smart positioner allows testing to be done more frequently. Typically the partial-stroke test moves the valve 10% from its original position, but it can be up to 30% if allowed by plant safety guidelines. Even though partial-stroke testing does not eliminate the need for full-stroke testing, which is required to check valve seating etc, it does reduce the required full-stroke testing frequency to the point where it can most likely be tested during plant turnaround.

The smart positioner provides diagnostic as well as positioning information, allowing the valve status and response time to be monitored during the test. Valve performance trends can be monitored and analysed after each partial-stroke test so that poten-

tially failing valves can be identified long before they become unavailable.

The results of a signature test (Figure 1) can identify packing problems (through friction data), leakage in the pneumatic path to the actuator, valve sticking, actuator spring rate and bench set. The smart positioner stores this data for subsequent use. For instance, overlaying the results of a current signature test with those of previous tests can indicate if valve response has degraded. Corrective action can be scheduled, which ultimately increases valve availability and ensures that the valve responds upon demand.

Some smart positioners can alert the operator if a valve is stuck. As the positioner begins the partial-stroke test, it continually checks valve travel to see if the valve is responding properly. If it is not, the positioner will abort the test and alert the operator that the valve is stuck. This prevents the valve from slamming shut, should it eventually break loose. As an added safety advantage, should an emergency shutdown demand occur during testing the smart positioner will override the test, moving the valve to its safe position.

Installation

A smart positioner can be used with any control valve style, including sliding-stem, rotary, quarter-turn etc, with spring-and-diaphragm actuators, spring-return piston actuators, or double-acting piston actuators. Two types of installation are possible. Both use a solenoid valve and provide a redundant pneumatic path (the actuator pressure will always exhaust to allow the valve to move to the safe position). If the solenoid valve fails, the actuator pressure exhausts through the pneumatic path in the smart positioner. If the smart positioner fails, the actuator pressure exhausts through the solenoid valve.

Figure 2 shows a smart positioner installed in a four-wire system. In this installation the logic solver provides two separate outputs: a 4 to 20mA dc signal for the smart positioner and a 24V dc signal for the solenoid valve. The 4 to 20 mA output serves as the primary valve position control signal. It also is used to control the valve position during remote online partial-stroke testing.

The HART digital information is superimposed on the analogue signal, which means the same wire pair provides both the means to control the valve through the SIS and to monitor valve diagnostic information con-

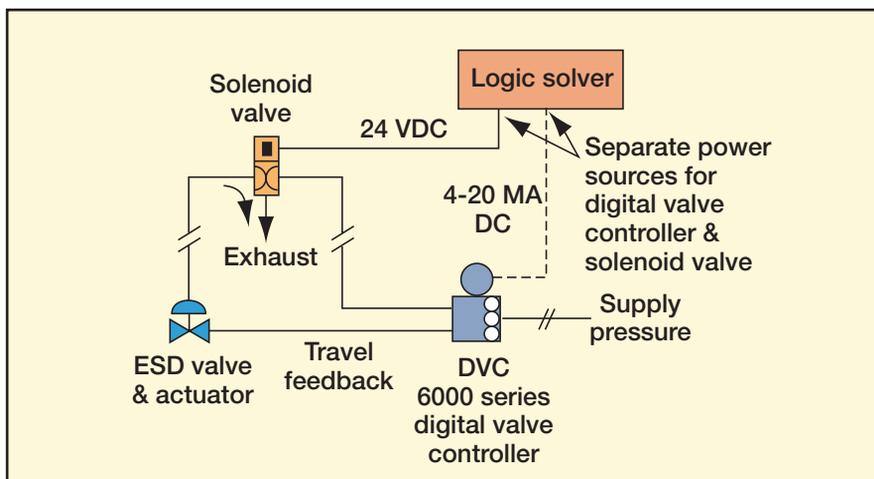


Figure 2 SIS schematic with a smart positioner in a four-wire system

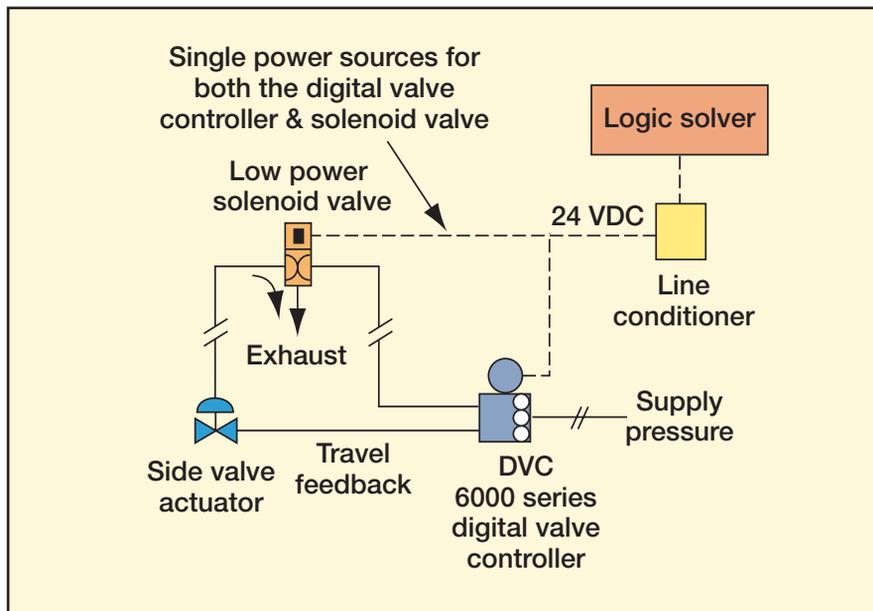


Figure 3 SIS schematic with a smart positioner in a two-wire system

tained in the HART signal. The second output from the logic solver, the 24V dc signal, is connected to the solenoid valve. It serves as an independent means of sending a SIS command to the safety valve. Consequently, two separate SIS signals are provided to the valve, permitting a one-out-of-two, fail-safe command.

The four-wire system requires an additional pair of wires, but it does permit the smart positioner to continue communicating even during "Safety Demand" conditions. Because the positioner continues to communicate, it can provide valuable trending information through its companion software. Being able to record the valve action during the emergency shutdown is very important for insurance or plant environment authorities since it provides evidence that the valve did stroke upon demand.

Figure 3 shows a smart positioner installed in a two-wire system. The logic solver powers both the solenoid valve and the smart positioner, which reduces wiring

costs in new installations and requires no additional wiring in existing installations. It also saves an I/O card in the control room. The installation, however, does require a line conditioner and a low-power solenoid valve. Because power is removed from the positioner during a demand, it will be unable to continue to communicate.

Conclusion

While the smart positioner provides performance and safety benefits through automated, online partial-stroke testing, many additional benefits can be realized. These include eliminating expensive pneumatic test panels, reducing manpower requirements, lowering base equipment cost and shortening testing time. In addition, remote testing results in fewer maintenance trips to the field as well as the establishment of an automated test routine that can produce great time savings.

Smart positioners allow partial-stroke testing while the process is running with no

threat of missing an emergency demand. This type of test applies a small ramp signal to the valve that is too small to disrupt the process, but is large enough to confirm that the valve is working properly. Installing the smart positioner along with a solenoid valve provides an inherently redundant pneumatic path. Should an emergency condition arise, the actuator pressure will always exhaust, either through the solenoid valve or through the smart positioner itself, thus ensuring that the valve will always go to the safe position.

The smart positioner can be designed so that it does not completely exhaust the actuator pressure should the valve become stuck during a partial-stroke test. This ensures that if the valve then becomes unstuck, it will not slam shut. The smart positioners would then abort the test and send an alert to the operator warning that the valve was stuck.

Smart positioners prove to be a great aid to predictive maintenance by providing a valve degradation analysis, which is important for critical valves in safety-related systems. This also reduces the amount of scheduled maintenance. The smart positioner provides a time and date stamp on all tests and reports, which is very important for complying with the requirements of statutory authorities. It also provides the capability for comparing and interpreting diagnostic data.

All in all, considering these unique benefits, the use of smart positioners in safety instrumented systems is a sensible and economical pathway to enhanced SIS reliability.

The authors work for Fisher Controls International Inc, of Marshalltown, Iowa, USA. Riyaz Ali is development manager for Fieldvue Business and LeRoy Jero is the company's publications specialist.



D351027X012 / 5M / 4 / 03

